우분투 보안

Denyhosts

계속된 침입이 발견되면 자동으로 해당 IP를 차단한다.

```
$ apt-get install denyhosts
```

특별히 해주어야 하는 설정은 없다.

Fail2ban

로그에서 주기적으로 정규표현식을 이용하여 의심스러운 ip를 찾아낸다. 그리고 해당 ip를 방화벽에 등록하여 자동으로 차단한다.

설치

```
$ apt-get install fail2ban
```

설정

`/etc/fail2ban/jail.conf` 파일을 편집한다. 알아두어야 할 옵션은 다음과 같다.

ignoreip	규칙을 무시할 ip와 Network을 설정한다.
bantime	검출된 ip를 방화벽에 등록하여 접속을 차단할 기간을 초 단위로 설정한다.
maxretry	정규 표현식으로 검사했을 때, maxretry에 설정한 횟수만큼 matching 되면 해당 IP를 방화벽에 등록한다.

참고

- 공식 사이트
- 나스위키

웹서버 DDOS 방어

여기서는 아파치의 mod_evasive 모듈을 이용한 DDOS 방어 방법을 정리한다.

설치

```
$ apt-get install libapache2-mod-evasive
```

로그가 저장될 디렉토리 생성

```
$ mkdir /var/log/mod_evasive
$ chown www-data:www-data /var/log/mod_evasive/
```

설정

다음과 같이 설정 파일을 만든 후 내용을 입력한다.

```
$ vim /etc/apache2/mods-available/mod-evasive.conf
```

```
<ifmodule mod_evasive20.c>
  DOSHashTableSize 3097
  DOSPageCount  2
  DOSSiteCount  50
  DOSPageInterval 1
  DOSSiteInterval  1
  DOSBlockingPeriod  10
  DOSLogDir   /var/log/mod_evasive
  DOSEmailNotify  email-address
  DOSWhitelist   127.0.0.1
</ifmodule>
```

모듈 활성화

```
$ a2enmod mod-evasive
```

이후 아파치를 재시작하면 된다.

참고

Ubuntu Server의 보안을 위해서 해야 할 것들
위 링크 정리

From:
http://obg.co.kr/doku/ - **OBG WiKi**

Permanent link:
http://obg.co.kr/doku/doku.php?id=linux:ubuntu:security

Last update: **2020/11/29 14:09**